



Why FastTips?

Wireless networking is the hottest buzzword in the IT industry today. Commercial and residential users want to cut the cord (the network cord) but keep linked to the Internet and other computer resources. However, until wireless networking protocols improve their security, our credit cards and corporate data are at risk. Anyone with a wireless receiver can access our data, even if they're invisible and a half mile away!

*Damar Group, Ltd.
PMB 451
6030-M Marshalee Dr
Elkridge, MD 21075
410.290.7000
1.888.290.6200
603.925.1110 (fax)
info@dgl.com
dgl.com*

Securing Your Wireless Network

A wireless LAN is the perfect way to improve data connectivity without installing extra cables and wire drops (wall jacks). It's also frees laptop users to roam around the building untethered; trips to the conference room, or a colleague's office can be made without losing touch with the network server, e-mail, or the web.

Home users find wireless networking a snap to set up and a big cost savings over conventional wired networks. A single cable or DSL modem can be shared by both the parents and the kids without any complex networking components.

But there's a hidden cost to wireless networking: security. The current wireless local area networking (WLAN) standard is 802.11. The most common implementation of this protocol, 802.11b (note the lowercase "b" in the designation) allows data that's transmitted from one computer to another or from a computer to the Internet to be encrypted while it's in the air. But any hacker worth her salt can find

free tools on the Internet to crack the encryption scheme of the 802.11b protocol. This isn't a big deal if you only use your home computers to surf the net and send e-mail to dear Aunt Sally, but it's a big concern if you don't trust your neighbors and you want to send your credit card to Amazon.com or LandsEnd.com. Your neighbors can pretty easily keep track of your transmissions even if your houses are separated by up to 2,000 feet!

This crack in the 802.11b security is especially worrisome if you're thinking about installing a WLAN in your office. You can probably think of a handful of competitors who'd pay a pretty penny for your network passwords, customer purchase history and your marketing list. Once you've logged into your network using an 802.11b wireless system, you've left your data open to anyone within a few hundred yards who cares to listen to your transmissions.

How do you fix this? Well, there's not a good alternative yet. Updated protocols, such as 802.11a and 802.11g, will be available soon, but until then, keep your data wired.

Wireless Security?

Most current products use spread spectrum technology. Vendors initially claimed it was difficult or impossible to de-spread or demodulate the signals. But they're wrong; it's actually easy to demodulate.

Spread spectrum technology uses an SSID (Service Set Identifier) as an identifier that's attached to each data packet passed over the WLAN.

Your network will be set to respond to only the SSID assigned to it, all other network SSIDs are ignored.

The problem is that SSIDs are sent in the clear, they're transmitted unencrypted. Software that's freely available on the Internet can pickup a network's SSID and allow an unauthorized user to send and receive data packets on your wireless network.

Many users think that just because their wireless network is rated for a maximum transmission range of 300 feet that they'll be safe, but actually all wireless access points can transmit up to 2,000 feet! The signal may be weak that far away, but it's still readable!